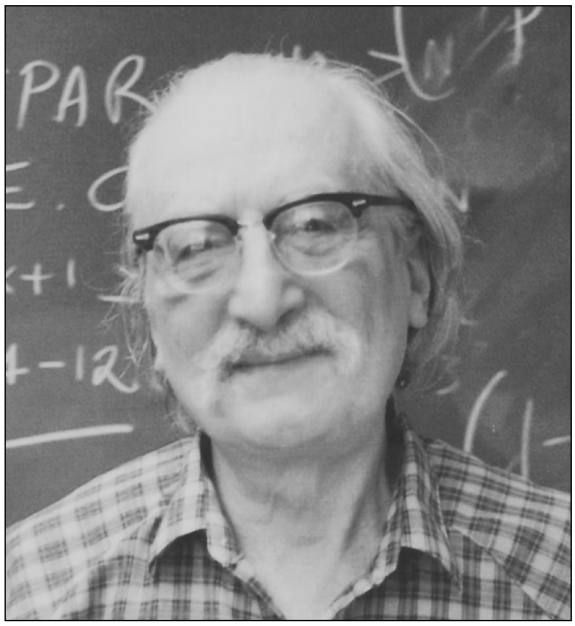
Daniel Shanks (1917–1996)

H. C. Williams

Daniel Shanks was born on January 17, 1917, in the city of Chicago, where he was raised and where in 1937 he received his B.S. in physics from the University of Chicago. In 1940 he worked as a physicist at the Aberdeen Proving Grounds, moving the following year to the position of physicist at the Naval Ordinance Laboratory, a position he retained until 1950. In 1951 his post at the NOL changed to that of mathematician, and during the years from 1951 to 1957 he headed the Numerical Analysis Section and then the Applied Mathematics Laboratory. He left the NOL in 1957 to become consultant and senior research scientist in the Computation and Mathematics Department at the Naval Ship R&D Center at the David Taylor Model Basin. In 1976 after support for independent work had considerably diminished, he decided to retire, spending a year as a guest worker at the National Bureau of Standards. He joined the Department of Mathematics at the University of Maryland as an adjunct professor in 1977 and remained there until his death on September 6, 1996. He is survived by two sisters; his sons, Leonard and Oliver; an adopted son, Gabriel; and two grandchildren.

Dan (he insisted that everyone call him Dan) received his Ph.D. from the University of Maryland in 1954, but it was as early as 1949, before having done any graduate work, that he presented his thesis to the somewhat surprised Department of Mathematics. It was at this point that he requested a Ph.D. in mathematics should the work be judged of sufficient quality. There was no question concerning the excellence of the work—indeed, the final thesis was little different from the original submission—but the University (as all universities will) insisted that he complete all their degree requirements before being awarded the degree. At the time Dan was raising a young family and working full time, so it was not until 1954 that he obtained his degree. His thesis was published in 1955 in the *Journal of Mathematics and Physics* and was entitled "Nonlinear Transformations of Divergent and Slowly Convergent Sequences". It concerned methods of accelerating the convergence of slowly convergent sequences and is now considered a classic in its field. The transformation that he introduced is today referred to as the Shanks transformation. Dan considered this paper to be one of his two most important published works.



Dan served as an editor of *Mathematics of Computation* from 1959 until his death. Throughout almost all of this period he was extremely active in all aspects of the journal's operation through his efforts in publishing his own work, soliciting papers that he regarded as being of particular significance, encouraging young mathematicians in their researches, reviewing tables, copyediting and even, when occasion demanded, serving unofficially in the capacity of managing

Hugh Williams is a professor in the Department of Computer Science at the University of Manitoba, Winnipeg MB, Canada. His e-mail address is Hugh_Williams@macmail.cs.umanitoba.ca.

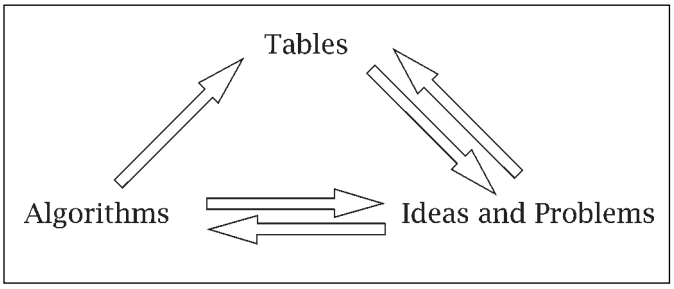


Figure 1.

editor. Many of his reviews of tables were sufficiently lengthy, detailed, and insightful to be research papers in their own right. He also served as the custodian of the UMT (Unpublished Mathematical Tables) file. Fortunately, this file, while no longer maintained by *Mathematics of Computation*, is temporarily being preserved for archival purposes through the generous efforts of Duncan Buell of the Center for Computing Sciences in Bowie, MD. It is hoped that a permanent home for the UMT will be found soon. In 1987 Dan was honored by the publication of a special issue of *Mathematics of Computation* dedicated to him on the occasion of his seventieth birthday and commemorating his many contributions to computational number theory. For it was in this area of research and related journal activities that he made his greatest contribution to *M of C*, a periodical which has now become the journal of choice for publications in both numerical analysis and computational number theory. This rather odd combination of areas was initiated through D. H. Lehmer's association with *M of C* at its very beginning in 1943, when it was called *Mathematical Tables and Other Aids to Computation (MTAC)*. That the number theoretic component of *M of C* has continued to flourish to this day is in no small part due to Dan's tireless efforts and his relentless insistence on the quality of the articles that appear in this journal.

Dan wrote over eighty papers and one book. The main areas to which he made contributions were: numerical analysis, distribution of primes, Dirichlet series, quadratic forms (fields), class group invariants, and computational algorithms in number fields of degree 3 and 4. He wrote as well on a variety of other topics, such as: black body radiation, ballistics, mathematical identities, Epstein zeta functions, formulas for π, and primality testing by means of cubic recurrences. Dan's papers are most frequently characterized by an experimental approach to their subject matter, likely as a result of his training as a physicist.

He illustrated his philosophy concerning this in a survey paper on algebraic number fields as shown in Figure 1. Here the arrows signify the connection between the various topics. For example, "ideas and problems", which are of the greatest interest mathematically, motivate the construction of tables and are frequently inspired from the examination of tables.

His early work (1951–58) was mainly devoted to numerical analytic topics, interests which led in 1962 to his most famous paper. This is his work with John Wrench on the computation of π to 100000 decimals, a considerable improvement over all previous work on this problem. Several new ideas for effecting such large-scale computations were mentioned in this paper, but Dan never seemed to have regarded it as highly as several of his later works. It should also be mentioned that in 1962 he published the first edition of his book *Solved and Unsolved Problems in Number Theory*. This is a charming, unconventional, provocative, and fascinating book on elementary number theory which has seen three further editions, the latest in 1993. It is the second of his works of which Dan was most proud.

Dan's earlier investigations in number theory began with his interest in the distribution of primes. In particular, he studied primes of the form n^2+a, n^4+1, and n^6+1091. In the last case he found that there was only one prime of the form n^6+1091 for $1 \le n \le 4000$ and gave a heuristic explanation as to why one would not expect to find many primes of this form. He developed a sieve technique to search for primes of the form n^2+1; a refinement of the same idea was used later by Carl Pomerance in his very successful quadratic sieve method for factoring integers.

If we let $P_a(N)$ represent the number of primes of the form n^2+a for $1 \le n \le N$ and $\overline{\pi}_a(N)$ denote the number of primes $\le N$ for which $-a$ is a quadratic nonresidue, then a conjecture of Hardy and Littlewood in 1923 implies that

$$(*) \quad \frac{P_a(N)}{\overline{\pi}_a(N)} \sim h_a,$$

where h_a is given by the very slowly convergent infinite product over the primes p

$$h_a = \prod_{p \setminus a} \Big(1 - \big(\frac{-a}{p}\big)\frac{1}{p-1}\Big)$$

and $(\cdot/p)$ is the Legendre symbol. Dan gave a heuristic argument in support of (*), ran a number of numerical experiments to verify (*) for N up to 180000, and developed a fast method to evaluate h_a. Indeed, he computed h_a for $a = 1$, ± 2, ± 3, 4, ± 5, ± 6, ± 7 to 8 decimals and gave 3 decimal estimates of several others.

It was this study that led him to his work on Dirichlet series and class number computation for quadratic forms. For a given character χ the Dirichlet series is defined by

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}.$$

If $\chi(n)$ is the Kronecker symbol (d/n), then he showed that h_a could be given by formulas like

$$\frac{h_aL(1,\chi)L(2,\chi)}{\zeta(4)}=\frac{1}{2}\prod_{p|a}\left(1-\frac{1}{p^4}\right)\prod_{q\geq 3}\left(1-\frac{2}{q(q-1)^2}\right),$$

where $d=-a$ and the products are evaluated over the primes. Since $L(2,\chi)$ and the product on the right can be evaluated rather quickly, this leaves only the problem of evaluating $L(1,\chi)$ in order to find h_a. However $L(1,\chi)$ is given by

$$L(1,\chi)=\begin{cases}\frac{2\pi h}{w\sqrt{-d}} & \text{when } d<0,\\ \frac{2Rh}{\sqrt{d}} & \text{when } d>0.\end{cases}$$

Here w denotes the number of roots of unity in the quadratic field K$=Q(\sqrt{d})$, h is the class number of K, and R is the regulator of K.

Dan therefore turned his attention to the problem of computing R and h. When he began his study of how to compute these invariants, the best available algorithms were of complexity $O(\sqrt{|d|})$. These investigations into the development of faster algorithms for the determination of h and R form the basis of some of Dan's best work. He developed the baby-step/ giant-step method of computing h (CLASNO), a technique that was later proved by Lenstra and Schoof to be of complexity $O(|d|^{1/5+\varepsilon})$ under the Extended Riemann Hypothesis (ERH). Later he discovered that each individual class of indefinite binary quadratic forms of discriminant d possesses a kind of structure, which he called the "infrastructure" of the class. Dan took advantage of this observation to develop an $O(d^{1/4+\varepsilon})$ algorithm to compute R (REGULA). This algorithm was also shown later by Lenstra and Schoof to be of complexity $O(d^{1/5+\varepsilon})$ under the ERH. His discovery of the infrastructure greatly surprised Dan because Gauss, for whom Dan had the most profound and abiding respect, had not made this same discovery during his seminal investigation of the properties of forms. The infrastructure idea has since been generalized by Buchmann to all algebraic number fields, and it also is a significant component of the faster, subexponential algorithm (developed by Buchmann and his students) for finding R. As implemented by Cohen, Diaz y Diaz, and Olivier, this technique can now evaluate R for values of d between 40 and 60 digits.

Dan turned these investigations toward the problem of factoring integers. As he knew that the discovery of an ambiguous form of discriminant d could be used to factor d, it was simply a matter of finding elements of the 2-sylow subgroup of the class group of quadratic forms of discriminant $d(<0)$. His work resulted in a means of factoring d in $O(|d|^{1/4+\varepsilon})$ operations, a very good result at the time. He also showed how to use the theory of continued fractions to search for reduced ambiguous forms of positive discriminant d. He called this technique SQUFOF (square form factorization); it was very simple to implement (Dan's version ran on a hand calculator), was of complexity $O(d^{1/4+\varepsilon})$ and never operated on numbers greater than $O(\sqrt{d})$ to factor d. Unfortunately Dan never published SQUFOF, nor did he publish (CUFFQI) (cubic fields from quadratic infrastructure), a very clever algorithm for determining all the nonisomorphic cubic fields of a given discriminant. The papers describing these and other results exist only as uncompleted manuscripts.

This synopsis of Dan's work is all too brief, but I hope that it illustrates to some degree his major mathematical talent: the ability to elicit structure from what at first appears to be chaos. I would now like to devote some space to some comments on the kind of person he was. Although he could be a most formidable individual with little capacity to tolerate fools gladly, he was always most solicitous and encouraging of young researchers. He invariably expressed interest in their work and made great efforts to coax from them results of both quality and taste, for Dan's taste in mathematics was very highly developed. It is a great pity that he never took on any students. Dan maintained an enormous program of correspondence (more recently through e-mail) with many mathematicians wherein he prodded, questioned, and challenged, generating in the process much new mathematics. His manner in dealing with his peers, however, could often range from brusque to perfunctory, a characteristic that was not always found to be endearing. However, he very rarely intended any real offense to anyone and was often astonished and distressed that some of his remarks had been so interpreted. Dan will also be remembered for his sense of humor. No one in mathematics could tell a story quite the way he could; his rendition of even the most unfunny joke was often hilarious. Fortunately, his sense of humor also appears in his published work.

This, then, was Dan Shanks, a remarkably talented mathematician, an innovative editor, an indefatigable correspondent, an occasional cur-

mudgeon, and a marvelous raconteur. The world of mathematics, particularly computational number theory, is much poorer for his loss. I miss him enormously.

Selected Papers of Dan Shanks

These are the papers which Dan regarded as his best work.

[1] *Non-linear transformations of divergent and slowly convergent sequences*, Math. Phys., **34**, (1955), 1–42.

[2] *A sieve method for factoring numbers of the form* $n^2 + 1$, MTAC, **13**, (1959), 78–86.

[3] *Quadratic residues and the distribution of primes*, MTAC, **13**, (1959), 272–284.

[4] *On the conjecture of Hardy and Littlewood concerning the number of primes of the form* $n^2 + a$, Math. Comp., **14**, (1960), 321–332.

[5] *Generalized Euler and class numbers*, Math. Comp., **21**, (1967), 689–694.

[6] *On Gauss's class number problems*, Math. Comp., **23**, (1969), 151–163.

[7] *Class number, a theory of factorization, and genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, RI, 1971, pp. 415–440.

[8] *The infrastructure of a real quadratic field and its applications*, Proc. 1972 Number Theory Conf., (Boulder, Colorado, 1972), pp. 217–224.

[9] (with PETER WEINBERGER), *A quadratic field of prime discriminant requiring three generators for its class group, and related theory*, Acta Arith., **21**, (1972), 71–87.

[10] *New types of quadratic fields having three invariants divisible by 3*, Number Theory **4**, (1972), 537–556.

[11] *Systematic examination of Littlewood's bounds on* $L(1, x)$, Proc. Sympos. Pure Math., vol. 24, Amer. Math. Soc., Providence, RI, 1973, pp. 267–283.

[12] *The simplest cubic fields*, Math. Comp., **28**, (1974), 1137–1152.

[13] *Calculation and applications of Epstein zeta functions*, Math. Comp., **29**, (1975), 271–287.

[14] (with H. C. WILLIAMS), *A note on class-number one in pure cubic fields*, Math. Comp., **33**, (1979), 1317–1320.

[15] (with H. C. WILLIAMS), *Gunderson's function in Fermat's last theorem*, Math. Comp. **36**, (1981), 291–295.

[16] *Dihedral quartic approximations and series for* π, Jour. Number Theory, **14**, (1982), 397–423.

[17] (with WILLIAM ADAMS), *Strong primality tests that are not sufficient*, Math. Comp., **39**, (1982), 255–300.

[18] (with MORRIS NEWMAN), *On a sequence arising in series for* π, Math. Comp., **42**, (1984), 199–217.

[19] *Solved and unsolved problems in number theory*, first ed., Spartan Books, Washington, DC, 1962; 2nd, 3rd, 4th ed., Chelsea, NY, 1978, 1985, 1993.

[20] *On Gauss & composition I*, Number Theory and Applications, Kluwer Dordrecht, 1989, pp. 163–178.

[21] *On Gauss & composition II*, Number Theory and Applications, Kluwer Dordrecht, 1989, pp. 179–184.